A STUDY TO DETERMINE DAMAGE ASSESSMENT METHODS OR MODELS ON AIR FORCE NETWORKS

THESIS

LISA S. THIEM, Capt, USAF
AFIT/GIR/ENV/05M-18

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GIR/ENV/05M-18

A STUDY TO DETERMINE DAMAGE ASSESSMENT METHODS OR MODELS ON AIR FORCE NETWORKS

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Lisa S. Thiem, BS

Captain, USAF

March 2005

AFIT/GIR/ENV/05M-18

A STUDY TO DETERMINE DAMAGE ASSESSMENT METHODS OR MODELS ON AIR FORCE NETWORKS

Lisa S. Thiem
Captain, USAF

Approved:

/signed/	16 Mar 05
Dennis Strouble, PhD (Chairman)	date
/signed/	16 Mar 05
Summer Bartczak, Lt Col, USAF, PhD (Member)	date
/signed/	16 Mar 05
David Van Veldhuizen, Major, USAF (Member)	date

Abstract

Damage assessment for computer networks is a new area of interest for the Air Force. Previously, there has not been a concerted effort to standardize methods used for damage assessment or develop a model that can be applied in assessing network damage. This research attempts to identify if the Air Force MAJCOM Network Operations Support Centers (NOSC) or the Air Force Computer Emergency Response Team (AFCERT) use damage assessment models or methods. If they do use a model or method, an additional question of how the model was attained, decided upon, and trained for is asked. Additionally a question is asked to ascertain at what level network damage assessment should be performed. All information comes from interviews, via e-mail or telephone, of managers in charge of computer security incidents at the MAJCOM NOSC or AFCERT. Currently, there is some evidence to show that several organizations are using some form of network damage assessment; however, each organization has highly individualized damage assessment methods that have been developed internally. This uniqueness does not allow for the method or model used at one location to be used at another location without modifications. Also, since the method or model is unique to each organization, the results achieved by the method or model cannot be generalized and reproduced across the Air Force.

To My Husband, Mom and Children

Acknowledgements

I would like to express my heartfelt thanks to everyone who has contributed time and effort to this effort. They have all provided valuable support which has made this endeavor possible.

Special thanks go to my advisor, Dr. Dennis Strouble for his patience and understanding through the entire process. Without his help and guidance this thesis would not have been possible.

Additionally, much thanks go to LtCol Summer Bartczak and Major David Van Veldhuizen for acting as readers. Their attention to detail and thorough editing made this thesis better each time.

I must also thank those who acted as subjects during this process. They provided valuable insight and understanding into the damage assessment process the Air Force utilizes. None of this would have been possible without their willingness to help and answer questions or offer additional avenues to research.

Finally, my most profound thanks go to my husband, mother, and daughter for their extreme patience and understanding in getting through this process. It was not easy for any of us and deserves more than the simple recognition given here. Thank you for everything.

Lisa S. Thiem

Table of Contents

List of Figures

Figure

A STUDY TO DETERMINE DAMAGE ASSESSMENT METHODS OR MODELS ON AIR FORCE NETWORKS

I. Introduction

Problem Statement

The purpose of this study is to determine if the Air Force is using a damage assessment process when dealing with security "incidents" occurring on its networks or computers. This study attempts to determine what, if any, models or methods are currently used to accurately assess network damage that occurs when a network is hit by worms, viruses, hackers, malicious insiders, or other threats. It also attempts to determine how the models or methods work and how they were determined to be useful in damage assessment.

Definitions

The research being undertaken requires a common set of terms to be used by the reader to provide clarity and understanding. The terms defined include: damage assessment, information system, incident, and computer forensics.

For the purpose of this study an information system is defined as:

> The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. 2) All the electronic and human components involved in the collection, processing, storage, transmission, display, dissemination, and disposition of information. An IS may be automated (e.g., a computerized information system) or manual (e.g., a library's card catalog).
> (www.ciao.gov/ciao_document_library/glossary/I.htm: 2004).

The damage assessment definition used by CISCO Systems, a leading provider of network products, is: once an attack has been confirmed on a system or network, the initial portion of the remediation process will be damage assessment to determine the extent of damage the successful attacker caused on that system or network (http://business.cisco.com/glossary: 2005). Initially, this definition was useful since it discusses the extent of damage caused by an attacker to a network. However, this definition does not explain what form the damage assessment takes, whether it is a method or model that can be used by other organizations, or if it produces the same results each time it is applied to the same problem. For the purpose of this study, a modified definition of damage assessment is used. In this study damage assessment is defined as a method or model that can provide accurate, re-producible information about the tangible and intangible effects of a network attack (virus, hacker, insider, natural disaster). An incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability"(http://www.dfn-cert.de/eng/pre99papers/certterm.html: 2004). The definition of an incident may vary for each organization depending on many factors. The following are categories of incidents and examples that are considered generally applicable by the German Computer Emergency Response Team (CERT) who developed a Glossary of Computer Security Incident Handling Terms and Abbreviations to use when discussing incidents (http://www.dfn-cert.de/eng/pre99papers/certterm.html: 2004). The German CERT put together a glossary of common terms based on available documents from around the world, including Force Computer Emergency Response Team (AFCERT). The following

are definitions of types of incidents the German CERT have found and examples they use for clarification of the meanings

(http://www.dfn-cert.de/eng/pre99papers/certterm.html: 2004):

> * *Compromise of integrity*, such as when a virus infects a program or the discovery of a serious system vulnerability
>
> * *Denial of service*, such as when an attacker has disabled a system or a network worm has saturated network bandwidth
>
> * *Misuse*, such as when an intruder (or insider) makes unauthorized use of an account
>
> * *Damage*, such as when a virus destroys data
>
> **Intrusions*, such as when an intruder penetrates system security
>
> *(*http://www.dfn-cert.de/eng/pre99papers/certterm.html*:* 2004*).*

When an incident occurs and legal issues are raised in a court of law, forensics is the area concerned with developing evidence in criminal cases that can be used in a court. Not just any evidence, but evidence at the lowest, most rudimentary level of a criminal investigation. Forensics is much broader, though, than a tool to catch criminals. It is also used by organizations to find problems such as misuse of corporate property or time, misconduct, and attempted computer or network incidents. In 1991, the term "computer forensics" was coined by the International Association of Computer Specialists (IACIS) (NTI INC.: 2004). Computer forensics is also called network forensics, forensic computer science, media analysis, and network analysis (Yasinac, 2003: 15). For purposes of clarity, the definition used in this paper comes from a white paper put out by Technology Pathways. It says that computer forensics is "computer science in support of the law" (Brown: 2002). The nature of forensics is to develop information to be used in a

court of law. Brown's description appears to encompass all of the varied aspects of computer forensics and is still generic enough to allow for differences in types of incidents and methods of acquiring evidence. Electronic evidence is also a new term that has been defined as: "any record, data, file, source code, program, computer manufacturer specifications, and other imprint on a computer storage device" (www.computer-forensics: 2002). Electronic evidence is the output provided by a computer forensics investigation which can be used to convict a criminal or prove wrongdoing within an organization. Much can be drawn from computer forensics practices and tools that can be utilized in damage assessment.

Background

The Air Force defined information as a weapon/target in its publication *Global Engagement: A Vision for the 21st Century Air Force* (Department of the Air Force, 2003: 3). By redefining information in this way, the Air Force also redefined how the systems and networks upon which its information resides and travels are viewed. It has fostered the view that information is valuable to warfghter and to the enemies of warfighters. It also designated information as another way that battles can be fought and decide the outcome of a war.

In 1987, an astronomer named Cliff Stoll was assigned to the computer department at the University of California at Berkeley. His first assignment was to track down the cause of a 75 cent accounting error on the university's mainframe. Each minute of computer use was tracked and charged to an account, so the 75 cent discrepancy was out of place. What followed was one of the first documented cases where a criminal was hacking into government systems to steal information (espionage) (Stoll: 1989). At the

time, law enforcement and investigative agencies were not able to provide much support since their purview was either strictly military systems or required a crime involving $1,000,000 or more. Clifford Stoll's first well-documented attack in 1987 was only the first of many. The Air Force has continued to see attacks to its networks. The number of documented attacks on Air Force networks has climbed, sometimes causing extensive damage resulting in lost time and money. From 1992 to 1996, the number of intrusions into Air Force information systems rose from about 300 incidents to over 1400 (Department of Defense, 1996: 12). As of 2003, the number of incidents had risen to 5350 in Air Combat Command alone.

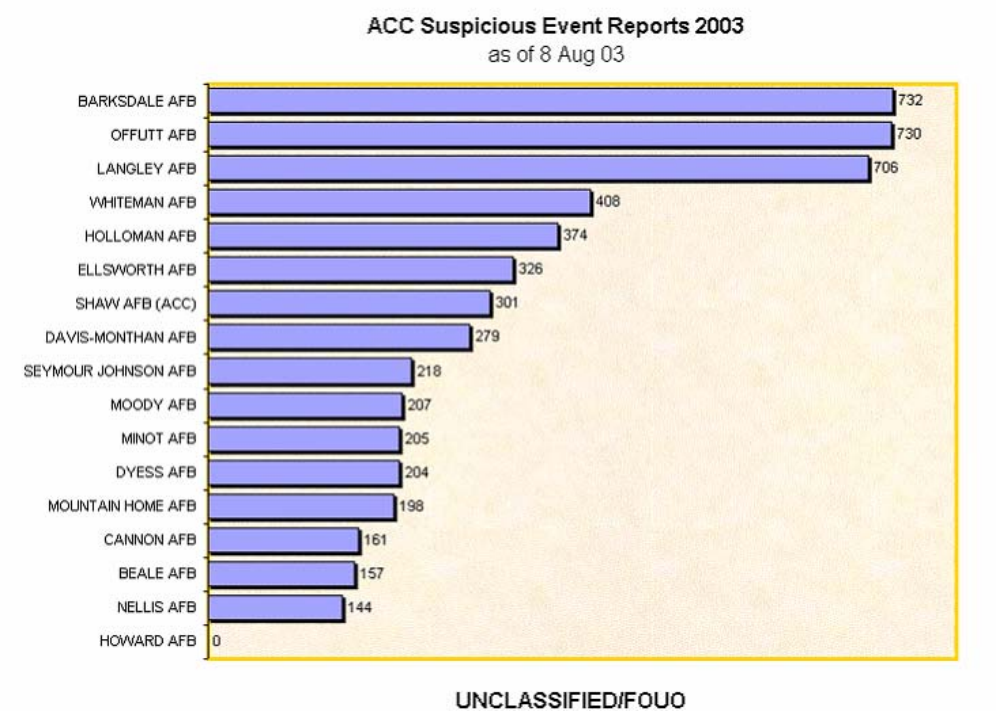

Figure 1 (https://www.my.af.mil/gcss-af/USAF/cms/AFMC/files/269,14,Slide: 2004)

The numbers, shown in Figure 1, represent a significant increase in a seven year period, but do not truly reflect the type and number of incidents the Air Force dealt with. For

example, there are likely to have been many incidents have gone undetected, as a large number appear to be something other than an attack, so they are not accounted for in the numbers shown (Conry-Murray, 2004).

As the data in Figure 1 shows, the number of suspicious events being reported is significant. In part, this is due to hackers and cyber-terrorists becoming more adept at wreaking havoc on systems, costing not only time and money, but possibly lives of personnel who rely on Air Force networks for accurate and timely data. Research into areas such as computer forensics, network vulnerability, and other fringe technology areas may help us to identify and eliminate these threats and keep Air Force information and people safer. It may also give AF investigators and prosecutors valuable tools in prosecuting perpetrators of these crimes while providing valuable information on the actual damage caused by incidents that can be used in building better networks. The data acquired can also be used to determine future budget needs in terms of acquiring new technology, provide an idea of the true worth of the information that resides on AF networks, and give a detailed assessment of damage caused by incidents in a time of war. Additionally, Air Force research must begin to delve into area of damage assessment on its networks.

Research Question

What is the AF currently using as a damage assessment method or model to assess damage (tangible and/or intangible) to its networks?

Investigative Questions

1.) Is the AF currently assessing damage to its networks caused by incidents?

2.) What method or model is the AF using to assess network damage or incidents?

3.) How does this method or model work?

Proposed Methodology

Due to the qualitative nature of this research, an interview approach will be used. Managers from Air Force MAJCOM Network Operations Support Centers (NOSC) and AFCERTwho are in charge of handling network or computer incidents will be interviewed to answer the research and investigative questions.

Scope and Limitations

This research delves into a relatively uninvestigated area; gaps in the knowledge as well as a lack of operational information or perspective are thus expected. Since this research is Air Force specific, it may have limited applicability to outside organizations. Another limitation to this research is the amount of time available to do a comprehensive look at the subject matter. In addition, researcher and interviewee bias is an issue since the research is subjective and hard to define. There are a limited number of participants which also presents itself as a limiting factor to the overall research.

II. Literature Review

Introduction

Exhaustive searches of the existing literature have shown that the focus of current research on network damage assessment is on tools to protect against network attacks or methods for handling evidence once an incident is identified. However, there is very little literature that looks at the true damage associated with computer network incidents. The most intense AF-related study on the subject matter was completed by Horony (1999). This is also a topic of interest in some commercial sectors, as found in the article by Conry-Murray (2002), but it is very limited and still a relatively new undertaking. In addition to the limited amount of existing literature concerning network damage assessment, there is also a problem with the term network damage assessment itself. Historically the term "damage assessment" has been used for assessing damage after a physical attack, such a dropping a bomb on a target, and not in reference to networks or computer systems, though, as shown by CISCO Systems definition this is changing.

Background and History on AF Networks

This section will describe the background and history leading up to the present day view of networks and their defense. It will review recent cybercrime statistics from the Department of Justice, the use of information warfare, and a case study from one of the first documented cases of computer espionage.

Cybercrime is the term used by the Department of Justice to address incidents that occur on computers and computer networks which it deals with. Cybercrime and the

attempts to prosecute it are in their infancy as shown by the Department of Justice statistics sections below:

> Data was collected for 2002 from 2,355 State court prosecutors who handle felony cases in State courts of general jurisdiction. During this time period, computer-related crimes (felony or misdemeanor) were prosecuted by 97% of full-time large offices, 73% of full-time medium offices, 44% of full-time small offices, and 17% of part-time offices.
> Three in ten offices nationwide reported prosecuting computer related crimes dealing with the transmittal of child pornography. A quarter of all offices prosecuted credit card fraud (27%) and bank card fraud (22%). Computer sabotage was prosecuted by 5% of the offices and theft of intellectual property by 3% (DOJ: 2003).

This commentary is a reflection of the current state of cybercrime convictions and focus of investigations handled by the Department of Justice. Cybercrime is the commercial terminology used in conjunction with computer or network related incidents. The AF discusses information warfare as well as cybercrime in its literature. Information warfare is seen as an entirely new form of warfare (Alberts, Gartska, Stein, 58: 2003). The military sees acts that the public sector calls cybercrimes as information warfare tactics that could be used to damage AF capabilities. Increasingly, there is concern about information warfare being used not only against military targets, such as AF networks, but commercial targets that provide essential infrastructure support such as electricity or commercial satellites used to transfer military information. These systems are considered to be more vulnerable than military targets due to the lack of security measures imposed on them, both internally and by governmental authorities (Berkowitz: 2000). Not only are these infrastructure assets more open and susceptible to viruses and indirect attacks, they are also playing key support roles to military networks by providing data storage, power, conduits for information, and other necessary functions (Berkowitz: 2000).

Foreign opponents will find these commercial targets more viable and easier to hit than purely military targets, and some of these efforts will come from countries who have long-term investments in time, money, and people to make these attacks successful (Berkowitz: 2000). Without network damage assessment, there is no method or model that will help the AF to understand how badly it has been impacted by an incident that has occurred, either directly or indirectly.

The technology now in place has changed drastically from the time of Clifford Stoll's *The Cuckoo's Egg* when system administrators had to be able to show a loss of $1,000,000 before the FBI would begin investigations (Stoll: 1989). There is a need, though, to look at Stoll's experiences as a case study for historical purposes and to gain knowledge from the past events that might have ramifications for current practices (Lee, 58: 1996). Historical information about computer incidents perpetrated over networks can hold the key to current problems as well as possibilities for understanding those problems (Lee, 59: 1996). History also provides valuable case studies that highlight vulnerabilities in networks and computer systems, which can be used as teaching tools as well as lessons for those who will follow (Lee, 61: 1996).

More recent events, such as the February 2000 distributed denial of service attacks that were launched against major U.S. corporations, are also important in teaching researchers and practitioners that new ways for network attacks to be launched are happening now. Evaluation of the network attacks might offer insight into predicting future attacks (Yurcik, Loomis, and Korcyk, 2: 2000). However, current methods used by system administrators to monitor and assess network health only address prediction of attacks, not how to assess the damage done by those attacks.

Network-Centric Warfare

With the rapid movement of the AF into the Information Age, network-centric warfare becomes more important and will require the use of network damage assessment methods to support it. Network-centric warfare is defined as:

> The conduct of military operations using networked information systems to generate a flexible and agile military force that acts under a common commanders intent, independent of the geographic or organizational disposition of the individual elements, and in which the focus of the warfighter is broadened away from individual, unit, or platform concerns to give primacy to the mission and responsibilities of the team, task group or coalition (Fewell and Hazen: 2003).

This new concept of how the Department of Defense uses its information technology will also require a more accurate way to estimate the damage done to its computer network assets. Since all elements of the force will be networked together, the vulnerability to network attacks increases (Fewell and Hazen, 2: 2003). A key element of the definition of network-centric warfare is the focus on network-centric thinking and effectively networking the "warfighting enterprise" (Alberts, Gartska, Stein, 86: 2003). This concept means that communications over networked platforms will be crucial to securing the battlefield and providing battlespace awareness of geographically separated entities to the warfighter (Alberts, Gartska, Stein, 86: 2003). Historically, geographically separated forces were weak and vulnerable (Alberts, Garstka, Stein, 90: 2003), but with the use of network-centric principles this has changed. Now information can be relayed almost simultaneously via networks as events occur to a variety of sources, such as ground units, naval warships, coalition allies, and AF planes in the air. Unfortunately, the changes also bring new dangers from data loss or theft, alteration of data that is intercepted by enemy

forces, and communication failure due to networks that are not functioning. These dangers must be acknowledged and addressed.

Why Damage Assessment Is So Important

This section will explain the background for using damage assessment on AF networks. Several AF documents were reviewed to find pertinent and timely data on the AF perspective of network damage assessment.

AF Policy Directive 33-2, *Communications and Information: Information Protection* (1996), lays the groundwork explaining who is responsible for different actions associated with the AF Network. It also provides a glossary of key terms used by the AF when discussing its networks; however, it overlooks assessing damage to AF networks, but focuses instead on network security and setup. Though this policy directive is dated 1996, many things have happened to change the face of networks and how they are secured and handled. AF Policy Directive 31-4, *Information Security* (1998), deals with Information Security. Again, this directive is outdated, but it is the most current version being used. It deals primarily with securing classified information, but it does not address the issue of how to assess the amount of damage that occurs to Air Force networks when information is compromised.

Air Force Doctrine Document 2-5, *Information Operations* (2003), discusses information operations (IO) and how they are "integral to all AF operations." This document focuses on IO and its employment of the core capabilities of influence operations, electronic warfare operations, and network warfare operations (AFDD 2-5, 1, 2003). It highlights information superiority as a critical part of air and space superiority which give commanders freedom from attack (AFDD 2-5, 1: 2003). However, it does

not mention how commanders are supposed to deal with network attacks should they occur. In all of the AF instructions and documents reviewed, the topic of how to accurately assess network damage is not addressed.

Current Research on Network Damage Assessment

In 1999, an AFIT student undertook the task of developing a model for damage assessment of computer security incidents. He found that there was no previous research to build on (Horony, 6: 1999). Despite this lack of foundation, he built the model shown (Figure 2), which is the only model of its kind that could be found.

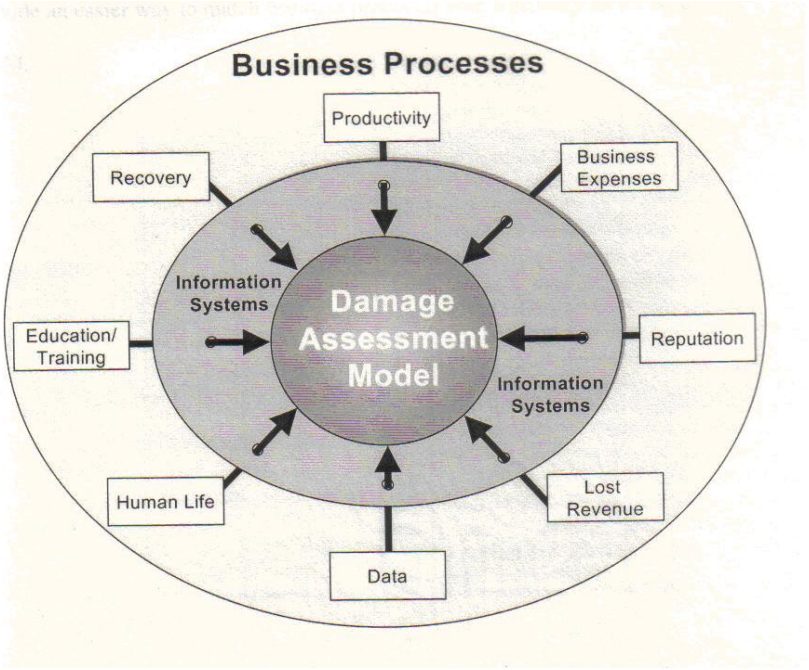

Figure 2 Damage Assessment Model (Horony: 1999)

Horony used a qualitative method of gathering data related to computer incident damage assessment (which also included networks), by interviewing subject matter experts (Horony, 26: 1999). This model provides a very top-level view of the areas that Horony found significant. These areas should be looked at in a computer incident damage

assessment model, but it does not offer specific avenues to performing damage assessment. This model provides a starting point for developing methods or models for network damage assessment, but it requires refinement to make it truly usable for executing specific actions.

The public sector looks at network damage assessment in terms of financial costs. A recent article in *Network Magazine* (Conry-Murray: 2004) discusses the problems associated with "tallying the costs of security incidents." This comment gives a good explanation of the need for damage assessment on networks of any kind. It says:

> Estimating the costs of intrusions, defacements, virus infections, and so on helps shape annual security budgets. Losses attributed to computer crime will affect revenue statements. Companies that want to report the crime to law enforcement, or file a civil suit, must also determine an incident's financial impact. Judges will demand hard numbers to help determine sentencing and restitution, and any sums cited by plaintiffs are sure to be attacked by defense (Conry-Murray: 2004).

Though there are other issues that are important to organizations in the public sector, such as reputation, ultimately, the financial costs are the driving force in attempts to use network damage assessment.

Link Between Damage Assessment and Computer/Cyber Forensics

The field of cyber forensics is relatively new though there are many white papers available from private companies who offer evidence gathering services for a fee. Cyber forensics has very close ties to the concept of network damage assessment since the work done using cyber forensics can provide valuable information that can be used in making network damage assessments.

Computers and networks have become the targets of modern cat burglars. They contain a vast amount of wealth in terms of information and data that is extremely sensitive and can cause empires to crumble if lost. In the last 15 to 20 years, computer forensics have become a valuable tool in protecting information wealth, or at least finding the perpetrator of the "crime".

Since computer forensics is still a new and developing science, the procedures being used to gather electronic evidence have come under intense scrutiny. Due to the seemingly endless uses that are being found for computers, computer forensics is rapidly expanding so that "electronic evidence" can be handled in a manner that allows organizations make decisions based on evidence rather than suspicion or circumstantial evidence.

Computer forensics has become increasingly important to organizations, both government and private. The increase in unauthorized computer users, internal espionage, cyber terrorism, and cyber crime all make the use of computer forensics vital to organizations by providing a much needed way to gather data after a computer or network incident and by providing the data necessary to conduct network damage assessment. In 2002, a survey completed by Computer Forensics Inc., a consulting firm that specializes in computer forensics, showed the seriousness of computer intrusions:

90% of respondents detected computer security breaches

80% acknowledged financial losses

44% of respondents reported losses of less than $500M

40% detected penetration from outside the network

40% detected penetration from inside the network
(Juhnke, 2002: 1-2)

Considering the amount of information that is kept on computer systems and how much that information is relied upon, the numbers above are important. People with malicious intentions have only to gain access to the target system to cause massive damage. They could even bring a halt to essential information-based infrastructures such as electrical grids, hospitals, or air traffic control systems as can be seen by Figures 3 and 4 there have been many attacks on AF systems. At the time of the attacks, 1993, the terminology used by the AF was different. Uncontrolled incidents were ones that were not caught until damage had already been inflicted on the systems. Malicious logic is the term used for worms, virus, and trap doors that cause damage to information systems.

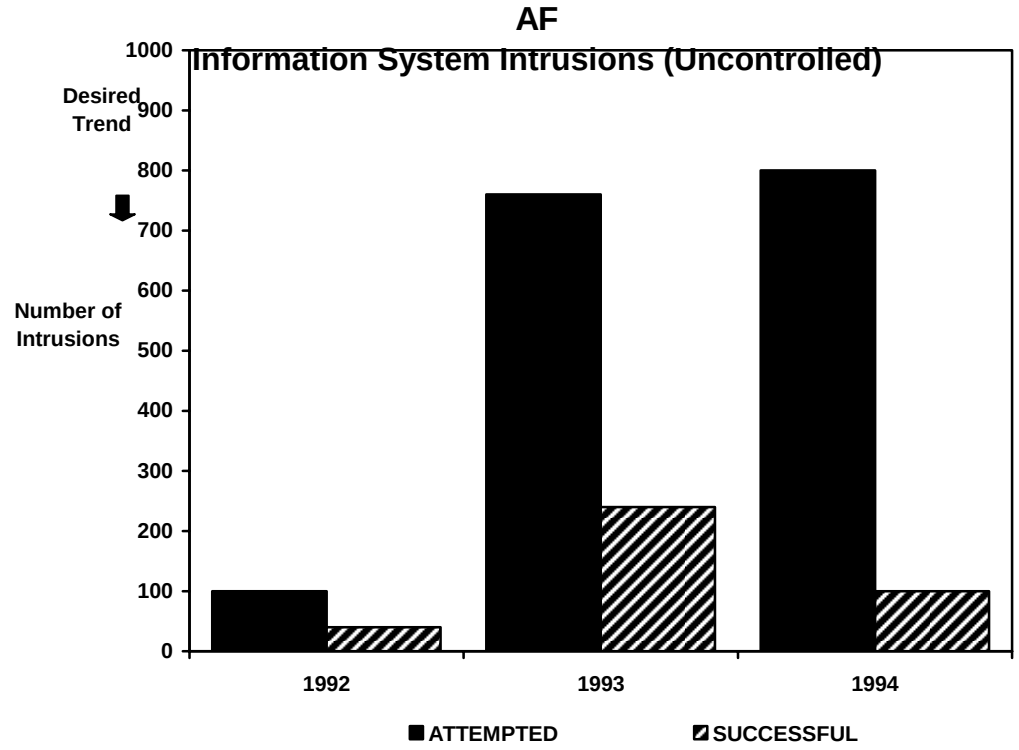

Figure 3 AF Information Systems Intrusions, 1993 (AFMAN 33-270*:* 1993)

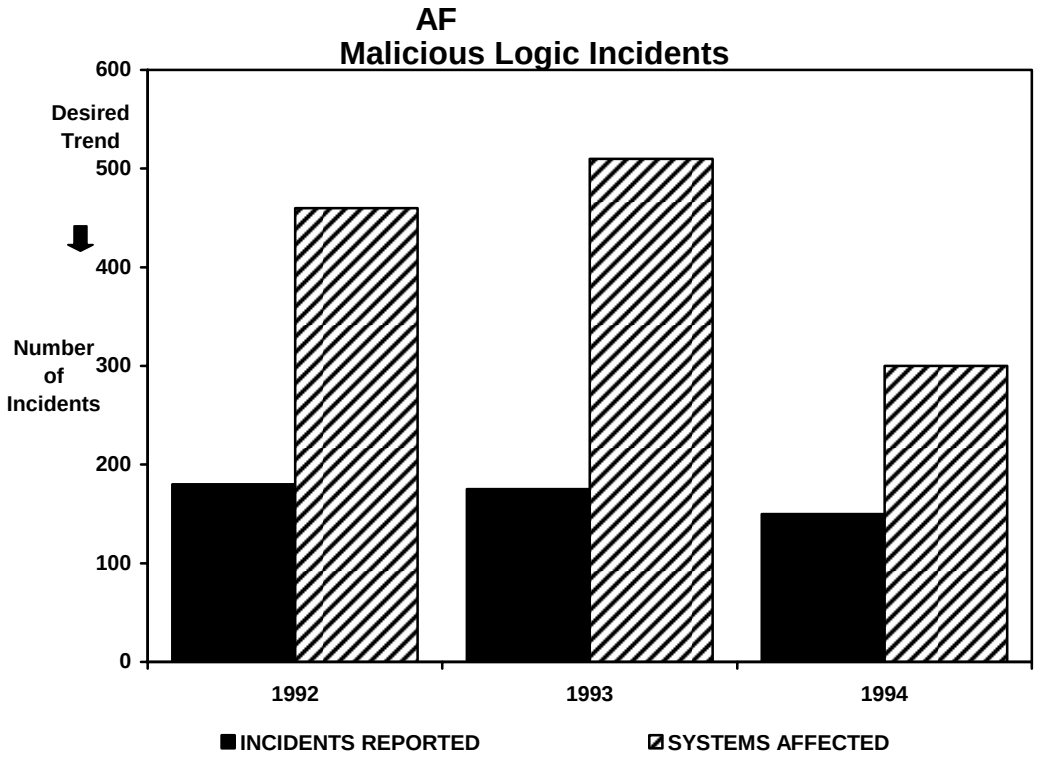

Figure 4 AF Malicious Logic Incidents, 1993 (AFMAN 33-270: 1993)

One of the keys to good forensic science of any kind is, “Do No Harm” (Juhnke, 2002: 4). First and foremost, this means that the investigator does not contaminate data important to the investigation, either inadvertently or purposefully. This becomes vitally important in computer forensics. Due to the volatility of the medium and the ease with which the “evidence” can be tainted, it is essential that computer evidence be treated in a systematic manner. However, there is no discussion found in the literature that addresses a systematic process for assessing the damage done by cyber criminals.

In a case where the criminal has used a specific computer as a portal onto a system, sometimes the computer has to remain untouched. It cannot even be removed from the network lest key evidence be lost. A computer forensics expert can safely gather information and ensure a secure chain of custody that will be useful in future litigation (Juhnke 2002: 4). Unfortunately, if the computer cannot be removed from the network, it (the computer) will still be vulnerable to the criminal who is using it. The first reaction of any system administrator is to secure the network, so educating the system administrators and users on what is required of them in case a network incident occurs is necessary for computer forensics to work.

Forensics experts find their evidence in one of three places generally. Evidence can be found on the perpetrator’s computer, on the “victim” computer, and on the network devices that have been affected (Desmond, 2000: 1). All of these items are easily tampered with, so a computer forensics specialist must be sure to maintain the integrity of the electronic evidence contained on a system.

The processes involved in conducting computer forensics are currently being standardized internationally through the use of the International Standards Organization

(ISO). This will help make computer forensics more reliable when used in network damage assessment. Specifically, ISO 17799 is "a comprehensive set of controls comprising best practices in information security" or, in other terms, a generic information security standard that can be universally applied which will give people working in computer forensics a common set of tools and practices to draw from (http://www.iso-17799.com: 2005). ISO 17799 was designed to "promote good practice for information security management" (Janes, 2002: 2). ISO 17799 addresses incident handling and the required skills to perform computer forensic investigations. ISO 17799 focuses on three major areas: protection of assets, vulnerabilities of assets, and human threats (Janes, 2002: 3-4). All of these areas are important and need to be addressed when assessing damage on AF networks because damage to one or all of these areas could lead to a loss of mission capability by AF warfighters.

Despite the relatively recent beginnings of computer forensics, it is rapidly becoming a part of organizations' information technology strategy and can provide a foundation for network damage assessment practices, methods or models. There are many people using a variety of techniques to gain access to data, bring down networks, steal trade secrets, corrupt or ruin information, or cause irreparable or catastrophic physical or logical damage to networks in whatever way they can. Computer forensics personnel are developing means to combat these threats through policy, software and hardware. Computer forensics is a growing science that will become increasingly important as society continues to automate and depend on technology and as organizations try to find ways to do network damage assessment. The key point of computer forensic science is to preserve the evidence (Takahashi, 2004: 74). When

assessing the damage to AF networks, the evidence is critical to finding holes and vulnerabilities that must be fixed. Electronic evidence also provides the background necessary for tracking the criminal (Takahashi, 2004: 76). Computer forensics will provide the groundwork for gathering the pertinent information when in-depth network damage assessments are required.

Summary

Network technology and network damage assessment is an area that the AF has taken an interest in. AF personnel have written several policy and guidance documents to ensure that AF networks run well and securely. However, there is no evidence in the existing AF instructions to show that the AF has looked beyond securing the network and closing any vulnerabilities that may occur. The field of computer forensics offers ways to gather evidence of the damage done by criminals who attack networks, but it currently does not address the problem of providing an accurate estimate of the damage caused.

III. Methodology

Introduction

This chapter outlines the methodology used to collect data and procedures for analyzing data used to answer the research questions. The research being done is qualitative research. An interview-based methodology was utilized to gain the maximum amount of information.

Methodology

Qualitative research is used to ". . . answer questions about the complex nature of phenomena, often with the purpose of describing and understanding the phenomena from the participants' point of view" (Leedy and Ormrod, 1985:101). This definition provides background that explains the reason a qualitative approach was utilized in this research. Qualitative researchers, unlike quantitative researchers, have generic questions with no clear variables, and collect large amounts of data from a small pool of subjects (Leedy and Ormrod, 1985: 101). The data collected is then organized and a verbal description is used to portray the situation that has been studied" (Leedy and Ormrod, 1985:101). For purposes of this study, a qualitative approach was chosen to provide a description of the phenomena of damage assessment on networks and an interpretation of the data obtained through subject interviews (Leedy and Ormrod, 1985: 148).

The specific qualitative approach chosen was an interview with target subjects. Based on the extensive number of uses for interviews, the following description will be used in this research to define the use of the interview technique.

> Interviews provide in-depth information about a particular research issue or question. Because the information is not quantifiable (i.e., not amenable to statistical analysis), the interview often is described as a qualitative research method. Whereas quantitative research methods (e.g., the experiment) gather a small amount of information from many subjects, interviews gather a broad range of information from a few subjects. (http://www.rider.edu/~suler/interviews.html#whatis: 2004).

The current research being undertaken presents multiple challenges which lends itself to the interview technique. The subjects were anonymous; however, the interviews were carried out via telephone interviews and through e-mail. The subjects were subject matter experts in the area of computer incident response from Network Operations and Security Centers (NOSCs) that reside at the Major Command level and the Air Force Computer Emergency Response Team (AFCERT). Feedback was requested from the research subjects to ensure that information provided by the subjects was used appropriately by the researcher.

The interview questions focused on ascertaining if subjects use a damage assessment method or model to assess the level of damage that has been inflicted after a network incident and the training required to use the method or model. There were six interview questions (Appendix A) asked of each subject. These questions are aligned to the three investigative questions posed in Chapter I. All questions were open-ended in an attempt to gather as much information as possible without introducing interviewer bias.

Investigative question one was addressed by the first interview question: "Is the AF currently assessing damage to its networks caused by incidents?" The subjects were asked is your organization using some form of damage assessment. If they answered

"Yes", the subject then continued to the next question. If they answered "No," they were directed to a new question.

For the second investigative question, "What method or model is the AF using to assess network damage or incidents?" there were two interview questions asked. They were: "How did your organization decide on the damage assessment procedures/model being used?", and "How does this method or model work?" These questions attempted to gather as much data about how the damage assessment was being accomplished in an organization.

Finally, investigative question number three asked: "How does this method or model work?" There was one interview question which applied to this investigative question. The interview question asked: "Please describe the procedures you use in assessing damage (step-by-step)." The question was designed to gather detailed data about the procedures that made up the method or model being used by the subjects' organizations.

There were three additional questions that did not directly relate to one of the three investigative questions, but provided useful data to explain why a subjects' organization did not have a process or method to perform damage assessment or at what level of the Air Force subjects believed damage assessment should be performed.

Subjects

The subjects being interviewed came from MAJCOM NOSCs and AFCERT incident response or security branches. They were mid-level managers in charge of offices that handle computer security incidents. A total of 14 subjects were solicited from the six Major Command NOSCs (including the Air Force Reserve Center NOSC) as

well as individuals from the AF Cert (organization responsible for overall AF network security and health) to provide data for the research.

Procedures for Analyzing Data

The interview data was broken up by each research question. A table was created in which all of the questions were used as the headings with the subsequent subject answers placed in the appropriate box. This allowed the researcher to easily manipulate the interview data and take each question by itself for review. The interviewer's conclusions were put into paragraph format using the subjects' responses to the interview questions.

The hermeneutic method is an interpretive research method that attempts to understand phenomena through the meanings that people assign to them (Myers, 4: 1997). Basically, this method looks at the similarities and differences amongst the respondents' answers in an attempt to build an overall picture. The hermeneutic method is highly qualitative and leaves the researcher open to personal and subject bias plus the research lacks reproducibility. However, this method can be very useful when the data is limited and the research is new by allowing for a holistic view of issues (http://redesignresearch.com/pde-3.htm, 2005). The researcher chose the hermeneutic method because there was a limited pool of data available from the MAJCOM NOSCs and AFCERT due to the small number of personnel performing network damage assessment. Additionally, there was very little previous research into the area of network damage assessment and the hermeneutic method is appropriate when research is dealing with new phenomena.

In researching network damage assessment, the hermeneutic method can be used to understand network damage assessment by assessing the meaning assigned to it by people at AF MAJCOM NOSCs and AFCERT. The hermeneutic method is also useful as a method of interpretation of "non-structured" and "non formal" approaches for understanding and decision-making (Bannister, 5: 2004). Because the hermeneutic method is useful in interpreting non-structured data such as the responses given in the interview questions, it was chosen to allow the researcher flexibility in interpreting and deciding how to utilize the data provided by the subjects. Ultimately, hermeneutics is called the art or science of interpretation which is what the researcher has done with the data obtained from the interviews with the seven subjects (Carlisle and Olson, 1: 2005). Carlisle and Olson go on to say that the hermeneutic method "begins with clustering observations into groups, seeking cohesive, thematic unity among clusters" (5: 2005). The researcher does this by creating a table with all of the data then analyzing the data based on the similarities and dissimilarities contained within the subjects' answers.

Limitations

The research had several limitations. One concern was finding an adequate pool of subject matter experts in network damage assessment to provide enough information. The short span of time allowed for producing this research created an additional limitation. One final limitation was the hermeneutic method. Though it has gained popularity as a research method in information systems and associated research, it was still subjective in that it provided ample opportunity for researcher bias in the data analysis process.

Summary

The methodology to be used is interview based and has several limitations. The subject pool is small and they are being interviewed using open-ended questions to extract the maximum amount of information possible. The subjects are being pulled from a highly specialized group of Air Force professionals, to include civilians and contractors to obtain the pertinent information. The data will be laid out in a table in order to analyze it and attempt to build a picture using the hermeneutic method of where the Air Force currently is in the use of damage assessment or damage assessment models on networks. The hermeneutic method allows the researcher to analyze similarities and dissimilarities found in the data.

IV. Results and Analysis

Sample Demographics

There were seven subjects interviewed from four MAJCOM NOSCs and AFCERT. The breakout according to AF rank was: two enlisted (Staff Sergeant and Master Sergeant) from Air Materiel Command (AMC), one government contractor (United States Air Force in Europe), and four company grade officers (one from Air Force Materiel Command, two from AFCERT, and one from AMC). The average number of years of experience in network security or support per subject was 2.3 years with the range being 6 months to 8 years 2 months. All positions held were in MAJCOM NOSCs or AFCERT. Two of the seven positions were NOSC crew commanders, two were network technicians, one was an officer in charge Incident Response, one was a flight commander, and one was a senior network security analyst. Several MAJCOM NOSCs did not respond for unknown reasons. This lack of response is considered normal by Leedy and Ormrod (Leedy and Ormrod, 1985, 223). They attribute it to response bias which can be caused by a variety of factors including: subject's education level, interest in the topic, or other factors (Leedy and Ormrod, 1985, 223).

Assessment by research question

1.) Is your organization using some form of network damage assessment?

The data obtained from this question was yes or no answers. All respondents answered this question. Five of the seven answered yes, their organization was using some form of network damage assessment based on the definition given previously. Using the hermeneutic method to evaluate the answers from the five respondents, there

were several similarities, as well as several differences in the subject's assessment of whether their organization was using some form of network damage. Two respondent's answers differed in that they did not feel that their organization was using network damage assessment.

1.a) Please describe the procedures you use in assessing damage (step-by-step).

Similarities in damage assessment methods

The use of in-house checklists was noted in two of the five respondent's answers. Additionally, information gathering, such as garnering all of the details of an incident from the personnel involved and recording it form of reports that are used to make an evaluation was noted by two subjects. The information gathering was mentioned in one form or another in all five subjects answers. Completing a checklist was considered a form of information gathering by one subject, however, other subjects to not state that they use checklists for information gathering but rather as a part of the procedure, or information gathering is separate from filling out a checklist associated with network damage assessment.

Multiple software packages were also mentioned as tools that were used in damage assessment. These included Remedy, ASIM (Automated Security Incident Measurement), and IDS (Intrusion Detection System). All of the software tools were parts of a larger process incorporated into the damage assessment methods of the specific organizations. These tools were used to monitor the network for intrusions and alert the appropriate authority or to incidents reported from other organizations.

Differences in damage assessment methods

Only one of the five respondents mentioned using an AF instruction (AFI 10-206, *Operational Reporting*: 2004) as a basis for their damage assessment method. The AF instruction was used to define reporting procedures, such as damage assessment, to a higher authority which was not mentioned by name. All other procedures were generated in-house with no acknowledged guidance from AF, Department of Defense (DoD), or commercial sources. Part of the process of network damage assessment was the creation of After Action Reports which was used to annotate the information acquired from the incident.

Overall assessment of question 1.a

Though there appears to be several areas where the damage assessment methods overlap, there are also several key points that differ dramatically. Checklists and standard reporting or incident response procedures for assessing damage after an incident have occurred is one area where there were similarities noted by the researcher. Checklists and procedures that guide personnel step-by-step through a pre-determined process seem to be the method of preference of most of the organizations to complete their version of damage assessment. These checklists and procedures were developed in-house according the information provided by the subjects. A reliance on software as a tool to aid in damage assessment was noted among several of the five subjects.

However, only one organization appears to have based any part of their damage assessment method on existing AF or DoD instructions. Because of this lack of AF guidance, it is difficult to ascertain what other official guidance was being used to develop a damage assessment method at the other organizations.

Additionally, the two subjects who answered no to this question (Is your organization using some form of network damage assessment?) were also significant because they were from the same NOSC that had a yes answer. This could be because of a validity issue with the question or a situation internal to the organization such as the subject's who responded no were not a part of the network damage assessment process and so did not know it existed. Reporting to higher level authorities such as commanders or the AFCERT (by NOSCs) was also cited in several subjects' comments. Reporting was either to leadership or higher level authorities and was not part if all of the subjects responses.

1.b) How did your organization decide on the damage assessment procedures/model being used?

Five of the seven subjects responded to this question. Following the hermeneutic method, subject's answers were compared and contrasted to build a picture that explained how that subject's organization developed their existing network damage assessment model or method. One of the five subjects was unable to offer data that could be used based on his lack of knowledge in this area, therefore only four subjects' data was evaluated.

Similarities in damage assessment model selection

Three of the four respondents said they utilized outside agencies help in creating their procedures for damage assessment. These outside agencies included, but were not limited to: Air Force Communication Agency, AF NOSC, other MAJCOM NOSCs, AFCERT, and Regional Computer Emergency Response Teams. They did this by informally contacting other agencies to ask what procedures were

being used there. Two of the four respondents commented that guidance came from "higher authorities".

Dissimilarities in damage assessment model selection

One of the respondents noted that lessons learned and network exercises were valuable in developing their "procedures" for damage assessment. The exercises provided experience about how network attacks occurred and the kind of electronic evidence to look for when assessing the damage caused by an incident. However, the other three respondents did not mention this at all.

One respondent stated that he relied heavily on existing software (IDS) logs to assess the amount of damage; however, the subject also noted that this method was not foolproof since it only caught known suspicious activity.

Only one respondent said that their damage assessment method was developed from AF and DoD guidance. This differs from the other subjects' responses in the way it was developed by supporting existing procedures through AF guidance while the other subjects focused on developing in-house procedures based on information they acquired from outside agencies. This response stands out since the subject's organization did not rely on informal communication or guidance from "higher authority" to develop a procedure for network damage assessment.

Overall assessment of question 1.b

Overall, the decision making processes for developing network damage assessment procedures utilized by the four different individuals' organizations was drastically different, though there was some overlap. Many of the subjects' stated that they contacted other NOSCs or agencies responsible for network security;

however, there was no formal process for developing damage assessment procedures. Each subject's organization developed internal stand-alone procedures that were specific to their needs.

1.c) Does the damage assessment method your organization uses require special training? If so, what is it?

Of the seven subjects who responded, five answered this question. Using the hermeneutic method to look at the similarities and differences in responses led to a conclusion as to whether special training was required to perform damage assessment in the respondents' organizations.

Similarities in damage assessment training requirements

On the job training (OJT) for network damage assessment processes was mentioned in three of the five subjects comments. OJT was particularly important where specialized checklists or procedures were performed when an incident occurred.

Two subjects referenced additional specialized training that was required for anyone who would be performing damage assessment. This training included tips-n-tricks, as well as training on the OSI model, Linux, Unix, and other unique software or systems used in the organization. The subjects felt this training was important in executing their damage assessment processes because it gave them in-depth system knowledge that could assist them in the event an incident occurred.

Two of the subjects also mentioned an in-house certification process, either specific to network damage assessment or generic to the crew commander position, with training in network damage assessment as a subset or secondary portion of the

overall certification process. This certification was required before damage assessment could be performed.

Differences in damage assessment training requirements

There was no single form of training that all five subjects mentioned when discussing network damage assessment. Each organization had a unique training plan that identified areas that were required before an individual was allowed to work on the network. These training plans included learning specific operating systems and software programs. Specific forms of training on network damage assessment were not addressed by the subjects'. One of the respondent's training consisted primarily of learning how to handle a specific software program, ASIM, which is used to measure security incidents. Only one of the respondents mentioned a standardized program of training for all personnel who will be performing damage assessment. Another subject mentioned that a standardized training plan was being developed for network damage assessment.

Overall assessment of question 1.c

Network damage assessment training is significant to all five respondent's organizations; however, the training is drastically different in each one. The focus of network damage assessment training is formal in some and informal (OJT) in others. As seen in the previous question, all five organizations had a different training program for network damage assessment. OJT was the most common method used according to the responses given, but formal training was also mentioned in two of the responses. Certification on network damage assessment or on the crew commander position was also mentioned by several subjects; however, this

certification was based on criteria that only applied to their organization. It was also noted that there was a requirement in most of the organizations for specialized training, generally in operating systems or software, based on specific systems being used for network monitoring or network performance. Overall, there were several indications that specialized training was required for network damage assessment.

1.d) Have you found other damage assessment models or methods that are not currently being used by your organization? What are they?

Overall assessment of question 1.d

Only one of the five subjects who responded to this question said they had found other network damage assessment methods or models; however, he called them "new application programs" that were used by system administrators to "monitor system status". All other subjects responded "no" with no additional comments.

1.e and 2.a) At what level do you believe that network damage assessment can/should be performed: Base, MAJCOM, Service, and DoD? Explain.

All seven subjects answered this question. There were many similarities and differences found amongst the seven subject's answers.

Similarities in damage assessment performance level

Four of the seven respondents agreed that network damage assessment needed to encompass all levels of the computer network hierarchy from base level up to DoD. Two subjects believed that the responsibility for performing network damage assessment should be accomplished by system owners at each level. Two subjects commented that damage assessment was dependent on the type of attack,

but felt that the Office of Special Investigations (OSI) should be the one performing damage assessment at all levels.

Differences in damage assessment performance level

One subject said that damage assessment was the responsibility first of the system owner but he felt all levels shared responsibility "equally". This subject was unique in his view that all organizational levels should be involved in network damage assessment.

Overall assessment of question 1.e and 2.a

Overall, there seems to be consensus that each level (base, MAJCOM, AF, DoD) must perform damage assessment. However, there were two subjects that believed that the system owner at each level should be performing damage assessment. Comparatively speaking, it was clear that the majority of the respondents see a need for damage assessment to be done at all levels within the AF and up to DoD. However, there is no clear answer to who they believe has the ultimate responsibility for performing it.

2.) Do you see a need for a damage assessment model in your organization? Why?

Overall assessment of question 2

Only two respondents answered this question, and they were in agreement upon their answer. They saw no need for network damage assessment, and both felt that it would only create an additional workload for personnel responsible for maintaining network integrity.

Summary

There was no clear network damage assessment model used across the four NOSCs and AFCERT; methods or models used by each organization were developed in-house. Additionally, training was mostly developed in-house and differed greatly from

one organization to the next. There was some agreement (four of seven) among respondents about who should be performing network damage assessment, but it was not unanimous.

V. Discussion and Conclusions

Findings

The researcher asked the following research questions in Chapter I.

1.) Is the AF currently assessing damage to its networks caused by incidents?

2.) What method or model is the AF using to assess network damage or incidents?

3.) How does this method or model work?

The research undertaken attempted to answer each of these questions. Question one found that there was not an AF-level program for network damage assessment, but individual programs created by each NOSC. Each NOSC had developed a network damage assessment method or model that was unique to their location. There was some indication that AF has provided guidance for some locations. Overall, each organization did say they were doing network damage assessment when incidents occurred on their networks.

For question number two there was evidence that network damage assessment methods or models were being used when an incident occurred, but they were not all the same across all organizations. Additionally, the damage assessment methods or models being used were developed internally by each organization, so there was no standard method or model for damage assessment across the organizations studied. Also of note,

was that there are possibly different methods used to assess network damage within specific organizations based on the specific type of incident that occurs.

Finally, the answer to question number three depended on the organization. Each organization has developed a site-specific method or model to address damage assessment. Each method worked differently from the other organizations'. There was some evidence that similarities exist amongst the methods or models used by the organizations; however, this was not due to agreement among the NOSCs or AFCERT about one specific method or model. Given the fact that the organizations did not use the same guidance and were working in different organizations it was important that they developed similar, generic procedures to handle network incidents

Another finding that the researcher found to be significant was the reliance on software to do network damage assessment. This could pose a concern about the validity and reliability of the assessment being done for several reasons. Software is a valuable tool that can augment a damage assessment method or model as a decision support tool, but it should not be the focus of the solution. Software can be tampered with and often has bugs that do not show up until after the software is in use. Additionally, hackers are constantly working out new ways to get around software, either through existing vulnerabilities or new vulnerabilities introduced with patches or upgrades. Software can also introduce unnecessary complexity by adding another step into an existing procedure, or requiring in-depth training. Software can also add additional work requirements that are not needed in completing network damage assessment such as requiring constant monitoring or maintenance so that the software works correctly. One last concern with

relying too heavily on software is that the data it contains is only as good as the personnel who have access to it. This means that someone who is incompetent or who has dishonest motives can wreak havoc by changing or destroying data that an organization depends on to do network damage assessment. Once the data has been changed, the output used by the network personnel becomes unreliable and can cause misdirection of work efforts, a false sense of security, or a complete network breakdown.

An additional finding that should be noted is the lack of clarity regarding the responsibilities of specific organizations in doing network damage assessment. There is no agency or organization specifically responsible for doing damage assessment on AF networks. There is also no agreement at what level of the AF or DoD the performance of network damage assessment should take place.

Finally, a few additional factors were highlighted. One factor of note was the reliance on checklists to perform network damage assessment and "information gathering processes" such as reports created when an incident occurred. These reports were generated and used by the individual NOSCs or AFCERT to brief higher authorities such as commanders and other leaders. Multiple respondents noted checklists in their interviews, though each checklist was developed in-house. Finally, training on network damage assessment was noted as an area of importance. OJT was key in several organizations along with some form of certification on the crew commander position or network damage assessment. Again, training on damage assessment procedures was different from organization to organization.

Limitations

There were multiple limitations encountered during this research. The first is investigator bias. Another form of bias is response or non-response bias which happens when subjects choose not to answer a question or not to answer a question honestly (Leedy and Ormrod, 222: 1985). The last form of bias that posed a limitation to this study is sampling bias. The small subject pool added constraints to the amount of data available. There were also limitations in the number of possible subjects, as well as the ability to communicate and contact the required subjects. This led to sampling bias and has implications when generalizations are being made about the larger population. It is possible that the data collected only applies in the organizations that responded, and therefore is of no use to the AF as a whole. Also, there was a limited amount of time to complete the research which did not allow for as comprehensive a study as the subject requires. This will be addressed in the Recommendation section as a suggestion for future research.

It is important to note that three of the seven subjects interviewed were from the same MAJCOM NOSC. Also, there were five different job titles among the seven respondents. Both of these factors limit the overall validity of their answers.

The final limitation that is important to note in this research is that the interview questions used were not validated beforehand. This limitation leads to validity questions for the overall research since the definitions or interview questions used were not proven to answer the investigative questions posed by the researcher.

Recommendations

A standardized definition of network damage assessment created by higher authority such as DoD or Headquarters AF would benefit the AF when discussing the needs and requirements for damage assessment on its networks. Based on the comments that came back on training programs, the researcher recommends that a standardized class should developed for Basic Communications Officer Training (BCOT) or Advanced Communications Officer Training (ACOT) that would teach basics of network damage assessment as defined by the AF. Standardized instructions, policies, and procedures would also be valuable in defining the network damage assessment process and allow for consensus across all NOSCs and AFCERT.

Though in a general sense, there were a lot of similarities amongst the responses, there were also a lot of differences that led the researcher to the conclusion that the AF needs to look at standardizing network damage assessment processes and procedures into a common method or model. Without a standardized method or model for damage assessment, there is no clear answer to questions about the amount of damage caused to AF networks by incidents.

The subjects interviewed appeared to force their responses to match the definition given for network damage assessment, though it is possible they were mistaking network damage assessment with their existing methods for incident response. The researcher reached this conclusion by reviewing the checklists used by one of the NOSCs which were designed to deal with classified message incidents and computer incidents, not incidents occurring on the network. This tendency to force their responses to match the given definition for network damage assessment could be because the definition was too

general, leaving the subjects open to interpret it too loosely or liberally. Since there is not a current definition in use by the AF for network damage assessment, there is a lot of room for subjective interpretation.

Future Research

There are many areas associated with network damage assessment that deserve additional research. One suggestion for a future research project would be to validate Horony's model from Chapter II. It is the only model of its kind that was found in the literature review, but it has not been researched beyond the initial findings. Further validating the model by using it to evaluate case studies could advance the area of network damage assessment dramatically and offer a clear source for NOSCs and AFCERT to develop their damage assessment procedures and methods in the absence of clear guidance from DoD directives and AF instructions. Horony's model could easily be tested by taking existing cases of network incidents and attempting to use his model to assess the damage.

Another possible project for future research would be to take an existing damage assessment model (possibly battle damage assessment) used by the AF Intelligence community and attempt to apply it to computer or network incidents. It would give network damage assessment an operational flavor as well as provide a framework from which to begin assessing damage to networks. It could also expand the perspectives of warfighters and leaders when confronted with network incidents by providing a clear assessment of the amount of damage done to a network by an attacker.

One final suggestion for future research would be a longitudinal study over multiple years that look at AF NOSC's and AFCERT's network damage assessment

models and methods in an attempt to see how the processes evolve over time. This would offer insight as to how network damage assessment models and methods used by the AF change over time.

Summary

There is a significant evidence to show that network damage assessment is being accomplished, though it is being accomplished based on individual organizations' concepts of damage assessment, not on a standard model. There is no evidence that the AF as an organization is using one specific damage assessment or model. Rather, individual organizations within the AF are developing their own methods and models to perform network damage assessment.

Appendix A

Interview Questionnaire

All information is confidential and will only be used for this research.

Below are the definitions for damage assessment and incidents.

Damage assessment is defined in this study as a method or model that can provide accurate, re-producible information about the tangible and intangible effects of a network attack (virus, hacker, insider, natural disaster).

An incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.

Questions:

General Information:

Job Title_____

Time in Position_____

Questions:

1.) Is your organization using some form of damage assessment?

YES (go to question 1.a) NO (go to question 2)

1.a) Please describe the procedures you use in assessing damage (step-by-step).

_____

1.b) How did your organization decide on the damage assessment procedures/model being used?

_____

1.c) Does the damage assessment method your organization uses require special education/training?

YES NO

If so, what is it?

_____

1.d) Have you found other damage assessment measures that are not currently being used by your organization?

YES NO

What are they?

_____

1.e) At what level do you believe that damage assessment can/should be performed: Base, MAJCOM, Service, DoD?

Explain._____

2.) Do you see a need for a damage assessment model in your organization?

YES NO

Why?

_____

2.a) At what level do you believe that damage assessment can/should be performed: Base, MAJCOM, Service, DoD? Explain.

_____

Bibliography

"About the Center." Center for Education and Research in Information Assurance and Security. Web site, http://www.cerias.purdue.edu/about.php3 (2 Nov 99).

Air Force Computer Emergency Response Team (AFCERT). "Mission and POC." Web site, http://afcert.csap.af.mil/mission.html (8 Jun 99).

Amoroso, Edward. Intrusion Detection: An Introduction to Internet Surveillance. Correlation. Traps. Trace Back and Response. Sparta, NJ: Intrusion.net Books, 1999.

Anderson, Kent. "Intelligence-based Threat Assessment for Information Networks and Infrastructures." Global Technology Research. Inc. White paper, March 98.

Bannister, Frank. "Value Perception in IT Investment Decisions." Electronic Journal of Information Systems Evaluation, Volume 7, November 2004.

Berkowitz, Bruce. "Information Warfare: Time to Prepare," *Issues in Science and Technology Online*, 1-12 (Winter 2000). 17 May 2003

Brown, Christopher L. "Developing Corporate Policies in Support of Computer Forensics". Technology Pathways, Technical White paper. Web site, www.TechPathways.com, 2002.

Bureau of Labor and Statistics. 1998-1999 Occupational Outlook Handbook. Online Handbook. Web site, http://www.bls.gox oco ocos042.htm, November 1999).

Carlisle, Judith, and Olson, David L. "Hermeneutics in Information Systems." 2005.

CISCO Systems. Web site, http://business.cisco.com/glossary, 2005.

Corey, Peterman, and others. "*Network Forensic Analysis*," *IEEE*, 1089-7801, 60-66 2002.

CERT®/CC "Incident Report." Statistics on WWWeb page. Web site, http://www.cert.org/stats cert_stats.html, November 1999.

CERT. "Steps for Recovering from a UNIX Root Compromise." Web site, http://www.cert.org/tech_tips/root_compromise.html, April 1999.

Center for Computer Forensics. Web site, Www.computer-forensics.net, 2002.

Central Intelligence Agency. Website, Www.ciao.gov/ciao_document_library/glossary/I.htm, 2004.

Colkin, Eileen. "Grainger Sees E-Commerce Payoff." Information Week Online. Web site, http://www.informationweek.com/shared/printableArticle?doc_id=IWK 19990429 S000, April 1999.

Cooper, Donald R. and Schindler, Pamela S. Business Research Methods. Boston: Irwin/McGraw-Hill, 1998.

Dalton, Gregory. "E-Business Evolution." Information Week. 737: 50 (7 Jun 99).

Dane, Francis C. Research Methods. Pacific Grove, CA: Brooks/Cole Publishing Company, 1990.

Denning, Dorthy E. Information Warfare and Security. Reading, MA: Addison-Wesly, 1999

Department of Defense. Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. Joint Publication 6-0, 30 May 1995.

Department of Defense. Joint Doctrine for Information Operations. Joint Publication 3-13, 9 Oct 1998.

Department of Defense Cert. Web site, Www.dfn-cert.de/eng/pre99papers/certterm.html, 2004.

Department of the Air Force, *Command, Control, Communications, and Computer (C^4) Systems,* Washington: HQ USAF, 17 September 1993.

Department of Defense, *Computer Investigations Training Program*. Web site, http://www.dcfl.gov/DCITP, 2004.

Department of the Air Force. *Communications and Information: Information Protection*. AF Policy Directive 33-2 Air Force. Washington: HQ USAF, 1 December 1996.

Department of the Air Force. *Information Operations*. Air Force Doctrine Document 2-5. Washington: HQ USAF, 2003.

Department of the Air Force. *Global Engagement: A Vision for the 21st Century Air Force*. Air Force Policy Document. Washington: HQ USAF, 2003.

Desmond, Paul. "When Security Fails: Network Forensics can help you recover from a security breach and potentially catch the culprit." Network World, Inc. 2000.

DiDio, Laura. "Computer Crime Costs on the Rise," Computer World: 23-25, April 1998).

Dyson, Esther. "A Map of he Network Society." New Perspective Quarterly. 14: 25-28 Spring 1997.

Geis, Gilbert. "The Case Study Method in Sociological Criminology." A Case for the Case Study. Ed. Joe R. Feagin, Anthony M. Drum, and Gideon Sjoberg. Chapel Hill, NC: The University of North Carolina Press, 1991.

Government Accounting Office/Accounting and Information Management Division. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Report Series GAOAIMD-96-84. Washington: GPO, 1996.

Government Accounting Office/Accounting and Information Management Division. Information Security: Computer Hacker Information Available on the Internet. Report Series GAO/T-AIMD-96-108. Washington: GPO. 1996.

Hafner, Katie and Markoff, John. Cyber Punks: Outlaws and Hackers on the Computer Frontier. NY: Touchstone, 1992.

Hamilton, Caroline R. "Risk Management and Security," Information Systems Security, vol. 8. issue 2: 69-78, Summer 1999.

Harvey, Christopher. "CERT—Computer Emergency Response Team," Computer Networks and ISDN Systems. 23: 167-170, November 1991.

Himebrook, Leslie F. A Model For Determining Information to be Captured Regarding Unauthorized Computer Entry of an Air Force Compute System. MS thesis, AFIT/GIS/LAS/97D-1. School of Systems and Logistics, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, December 1997.

Horony, Mark D. *Information System Incidents: The Development of a Damage Assessment Model*. WPAFB: AFIT, 1999.

Howard, John D. An Analysis of Security Incidents on the Internet: 1989-1995. Ph.D. dissertation. Carnegie Mellon University, Pittsburgh PA, April 1997.

Internet Engineering Task Force. Site Security Handbook. RFC 2196. September 1997. "IT Capital Outlay Growing." Electronic News. 42: 48, December 1996).

Janes, Simon. "Ibas Computer Forensics" Ibas UK Ltd, 2002.

Juhnke, Deborah H. "Cyber Terrorism or Cyber Crime?," Computer Forensics Inc, 2002.

Kammer, Raymond G. Statement before the House Science Subcommittee on Technology, Web site, http://www.house.gov/science/kammer_062499.htm, June 1999.

Kratz, Martin P.J. "Canada's Computer Crime Laws: Ten Years of Experience." Information Systems Security: Facing the Information Society of the 21st Century. Ed. Sokratis K. Katsikas and Dimitris Gritzalis. London: Chapman & Hall, 1996.

Kvale, Steinar. Interviews : An Introduction to Qualitative Research Interviewing. Thousand Oaks, CA: Sage Publications, 1996.

Lawlor, Maryann. "Virtual Hackers Help Take a Byte Out of Cybercrime," *Signal*, 58: 41-44 (February 2004).

Lee, John A. N. "Those Who Forget the Lessons of History Are Doomed to Repeat It or, Why I Study the History of Computing", *IEEE Annals of Computing*, 1996.

Leedy, Paul D. and Ormrod, Jeanne E. Practical Research Planning and Design. Columbus, OH: Merrill Prentice Hall, 1985.

Martell, Duncan. "Survey Looks at Cost of Information Technology." Bloomberg News. Digital Newspaper. Web site, http://wwwcomputernewsdaily.com 26"?_092497_ 102206_10495.html, November 1999).

McCune, Jenny C. "How Safe is Your Data?" Management Review:, October 1998.

Merriam-Webster Online. Excerpt from online dictionary. Web site, http://www.m-w.com/cgi-bin/dictionary, November 2004.

Mosquera, Mary. "Computer Attacks Spreading." TechWeb. Digital Newspaper. Web site, http://www.techweb.com/wire.stor>- T\\'B 199M1 1 lsS(n>n3, November 1999.

Myers, Michael D. "Qualitative Research in Information Systems." Association for Information Systems, June 1997.

New Technologies Inc. "Computer Forensics Defined." Excerpt from first paragraph. Web site, http"//www.forensics-intl.com.

Ott, Jeffrey L. "Preparing for the New Millennium." Information Systems Security: vol. 8:3-6, Summer 1999.

Pascal, Blaise. "Great Books of the World: Pascal." Encyclopedia Britannica. 33. Ed. Robert Maynard Hutchins. Chicago: University of Chicago Press, 1986.

Pethia, Richard. "Testimony before the Permanent Subcommittee on Investigations." Web page at CERT®/CC. Web site, http://www.cert.org/docs/, June 1999.

Power, Richard. "1999 CSI/FBI Computer Crime Security Survey." Computer Security Issues & Trends, vol. V. no. 1. San Francisco, CA: Computer Security Institute, Winter 1999.

http://redesignresearch.com/pde-3.htm, 2005.

Rezmierski, Virginia and others. Final Report: Incident Cost Analysis and Modeling Project. Michigan: University of Michigan Press, 1998.

Roberts, Timothy. "Hackers getting new foe". The Business Journals. February 2004.

Ruben, Aviel D., Geer, Daniel and Ranum, Marcus J. Web Security Sourcebook. NY: John Wiley & Sons, Inc., 1997.

Rutrell, Yasin. "Think Twice Before Becoming a Hacker Attacker." Internet Week. 745: 30, December 1998.

Schwartz, Feffrey. "IT Healthy in Finance Arena." Information Week. 771: 19, July 1999.

Shulman, Richard. "Technology—Make Plans for E-Business." Supermarket Business. 54: 33-34, August 1999.

Sterling, Bruce. The Hacker Crackdown: Law and Disorder on the Electronic Frontier. NY: Bantam Books, 1992.

Stoll, Clifford. *The Cuckoo's Egg: Tracking a Spy Through a Maze of Computer Espionage*. New York: DoubleDay Dell Publishing Group, Inc, 1989.

Straub, Detmar W. "Coping With Systems Risk: Security Planning Models for Management Decision Making(nl)," MIS Quarterly, vol. 22. issue 4: 441-469, December 1998.

Takahashi, Ikuo. "Legal System and Computer Forensics Business." IEEE, 74-77, 2004.

"Technology." Journal of Accountancy. 187: 16-17, January 1999.

Toigo, Jon. Disaster Recovery Planning: For Computers and Communication Resources. NY: John Wiley & Sons, Inc., 1996.

Triendle, Robert. "Sony Restructures to Embrace Digital Economy." Research Technology Management. 42: 4-5, September/October 1999).

Trigaux, Robert. "Hackers: Hidden Dangers." Web site, http://www.sptimes.com/Business 61698 Hackers_third_in_a_s.html, August 1999.

"Using Interviews in Research." Www.rider.edu/~suler/interviews.html#whatis, 2004.

Vatis, Michael A. "Cybercrime, Transnational Crime, and Intellectual Property Theft." Statement before Congressional Joint Economic Committee, March 1998.

Vatis, Michael A. "NIPC Cyber Threat Assessment" Statement before Senate Judiciary Committee: Subcommittee on Technology and Terrorism. 6 Oct 99.

Velissarios, John and Santarossa, Roberto. "Practical security issues with high-speed networks," *Journal of High Speed Networks*, 8: 311-324 (1999).

Violino, Bob. "The Security facade," InformationWeek: 68-69 (21 Oct 96).

Yasinac, Erbacher, and others. "Computer Forensics Education," *IEEE*, 1540-7993, 15-23 (2003).

Yurcik, William,Loomis, David, and Krycyck Jr. "Predicting Internet Attacks: On Developing An Effective Measurement Methodology," *Proceedings of the 18th Annual International Communications Forecasting Conference*. 1-9. Seattle 2000.

Willemse, Nicolene and du Toit, Adeline S.A. "Determining the Value of Information— A Pragmatic Approach." South African Journal of Library & Information Science. 64: 8-14, March 1996.

Wright, Marie A. "The Need for Information Security Education." Computer Fraud & Security: 14-17, August 1998.

Vita

Captain Lisa S. Thiem graduated from Cimarron High School in Cimarron, Kansas. She entered undergraduate studies at Troy State University of Montgomery in Montgomery, Alabama where she graduated with a Bachelor of Science degree in Psychology in June 1998. She was commissioned through the Detachment 019 AFROTC at the Alabama State University.

Her first assignment was at the Air Force Research Laboratory, Human Effectiveness Directorate, Brooks AFB (now Brooks City-Base), Texas as a behavioral psychologist in January 1999. In December 2001, she was assigned to the 27th Communications Squadron, Cannon AFB, New Mexico where she served as communications and computer officer. In August 2003, she entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation, she will be assigned to the Air Force Research Laboratory, Human Effectiveness Directorate, Wright-Patterson AFB, Ohio.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
03-21-2005	**Master's Thesis**	Aug 2003 – Mar 2005

4. TITLE AND SUBTITLE

A STUDY TO DETERMINE DAMAGE ASSESSMENT METHODS OR MODELS ON AIR FORCE NETWORKS

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Thiem, Lisa S., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/05M-18

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFRL/HEC
Attn: Ms. Laurie Fenstermacher
AFRL/HECS, 2255 H Street, Bldg 248
WPAFB OH 45433-7765 DSN: 785-8882

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Damage assessment for computer networks is a new area of interest for the Air Force. Previously, there has not been a concerted effort to codify damage assessment or develop a model that can be applied in assessing damage done by criminals, natural disasters, or other methods of damaging a computer network. The research undertaken attempts to identify if the Air Force MAJCOM Network Operations Support Centers (NOSC) use damage assessment models or methods. If the Air Force does use a model or method, an additional question of how the model was attained or decided upon is asked. All information comes from interviews, via e-mail or telephone, of managers in charge of computer security incidents at the Major Command level. The research is qualitative, so there are many biases and opportunities for additional, more research. Currently, there is some evidence to show that several Network Operations Support Centers are using some form of damage assessment, however, each organization has highly individualized damage assessment methods that have been developed internally and not from a re-producible method or model.

15. SUBJECT TERMS
Network damage assessment, interview-based research, AF network

16. SECURITY CLASSIFICATION OF: UNCLASS			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Dennis Strouble, Ph.D., USAF (ENV)
U	**U**	**U**	**UU**	63	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 3323; e-mail: dennis.strouble@afit.edu

Standard Form 298 (Rev: 8-98)
Prescribed by ANSI Std. Z39-18